#3

Docket No. 1337.1028/MDS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Kyung-Hee KANG et al.

Serial No.: 09/735,921 Group Art Unit: Unassigned

Filed: December 14, 2000 Examiner: Unassigned

For: METHOD FOR MANAGING CERTIFICATE REVOCATION LIST BY DISTRIBUTING IT

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. §1.55

Honorable Commissioner of
Patents and Trademarks
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. §1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Korean Patent Application No. 2000-60053, filed October 12, 2000.

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. §119.

Respectfully submitted,

STAAS & HALSEY LLP

By: _____
Michael D. Stein
Registration No. 37,240

700 Eleventh Street, N.W.
Washington, D.C. 20001
(202) 434-1500

Date: 4/2/01

pooKA016

대 한 민 국 특 허 청
KOREAN INDUSTRIAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Industrial Property Office.

출 원 번 호 : 특허출원 2000년 제 60053 호
Application Number

출 원 년 월 일 : 2000년 10월 12일
Date of Application

출 원 인 : 한국전기통신공사
Applicant(s)

2000 년 11 월 10 일

특 허 청
COMMISSIONER

【서류명】 특허출원서
【권리구분】 특허
【수신처】 특허청장
【제출일자】 2000.10.12
【발명의 명칭】 인증서 폐지목록 분산 관리 방법
【발명의 영문명칭】 Method for managing dispersion certificate revocation list

【출원인】
【명칭】 한국전기통신공사
【출원인코드】 2-1998-005456-3
【대리인】
【성명】 특허법인 신성 정지원
【대리인코드】 9-2000-000292-3
【포괄위임등록번호】 2000-050018-1
【대리인】
【성명】 특허법인 신성 원석희
【대리인코드】 9-1998-000444-1
【포괄위임등록번호】 2000-050018-1
【대리인】
【성명】 특허법인 신성 박해천
【대리인코드】 9-1998-000223-4
【포괄위임등록번호】 2000-050018-1
【발명자】
【성명의 국문표기】 강경희
【성명의 영문표기】 KANG,Kyung Hee
【주민등록번호】 680727-2470614
【우편번호】 137-792
【주소】 서울특별시 서초구 우면동 17
【국적】 KR
【발명자】
【성명의 국문표기】 김선정
【성명의 영문표기】 KIM,Sun Jung
【주민등록번호】 680311-2063410

【우편번호】 137-792
【주소】 서울특별시 서초구 우면동 61 성우빌라 102호
【국적】 KR
【발명자】
【성명의 국문표기】 양성현
【성명의 영문표기】 YANG,Seong Hyoen
【주민등록번호】 730720-1235031
【우편번호】 137-792
【주소】 서울특별시 서초구 우면동 17
【국적】 KR
【발명자】
【성명의 국문표기】 임영숙
【성명의 영문표기】 LIM,Young Sook
【주민등록번호】 650313-2730411
【우편번호】 463-070
【주소】 경기도 성남시 분당구 야탑동 장미마을코오롱아파트 129-1101
【국적】 KR
【취지】 특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대리인 특허법인 신성 정지원 (인) 대리인 특허법인 신성 원석희 (인) 대리인 특허법인 신성 박해천 (인)
【수수료】

【기본출원료】	20	면	29,000 원
【가산출원료】	9	면	9,000 원
【우선권주장료】	0	건	0 원
【심사청구료】	0	항	0 원
【합계】	38,000 원		

【첨부서류】 1. 요약서·명세서(도면)_1통

【요약서】

【요약】

1. 청구범위에 기재된 발명이 속한 기술분야

본 발명은 인증서 폐지목록 분산 관리 방법과 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체에 관한 것임.

2. 발명이 해결하려고 하는 기술적 과제

본 발명은, 분배점 메커니즘을 적용하여 인증서 폐지목록(CRL)을 효과적으로 분산 관리하기 위한 인증서 폐지목록 분산 관리 방법과 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공하고자 함.

3. 발명의 해결방법의 요지

본 발명은, 인증서 폐지목록 분산 관리 시스템에 적용되는 인증서 폐지목록(CRL : Certificate Revocation List) 분산 관리 방법에 있어서, 상기 인증서 폐지목록의 분배 구간을 산출하여 상기 인증서 폐지목록에 대한 인증정책을 등록하는 제 1 단계; 상기 등록된 인증정책에 따라 가입자 인증서를 구성하는 구조체를 셋팅하여 인증서를 발급하는 제 2 단계; 상기 발급된 인증서 폐지목록에 분배점 메커니즘을 적용하여 상대방 인증서의 유효성을 검증하는 제 3 단계; 및 사용자의 인증서를 폐지하기 위하여 상기 인증서 폐지목록의 분배점을 이용하여 인증서 폐지목록을 갱신하고, 그 내용을 게시하는 제 4 단계를 포함함.

4. 발명의 중요한 용도

본 발명은 인증서 폐지목록 분산 관리 시스템 등에 이용됨.

【대표도】

도 4

【색인어】

인증시스템, 인증서 폐지목록(CRL), 분배점(DP), 해쉬함수, 서브젝트 네임(SUBJECT_NAME)

【명세서】

【발명의 명칭】

인증서 폐지목록 분산 관리 방법{Method for managing dispersion certificate revocation list}

【도면의 간단한 설명】

도 1 은 일반적인 디렉토리 서버의 인증서 폐지목록 관리 구조에 대한 예시도.

도 2 는 도 1에 적용되는 사용자 단말 환경에서 인증서 폐지목록을 이용한 상대방 인증서의 유효성 검증 과정에 대한 상세 흐름도.

도 3a 및 도 3b 는 ITU-T X.509 표준문서에서, 인증서 폐지목록에 분배점을 적용하였을때, 사용하도록 정의한 데이터 구조체에 대한 예시도.

도 4 는 본 발명이 적용되는 공개키 기반 구조 보안 서비스 시스템에 대한 구성예시도.

도 5 는 본 발명에 따른 인증서 폐지목록 분산 관리 방법 중 인증시스템의 인증정책 등록 과정에 대한 일실시예 흐름도.

도 6 은 본 발명에 따른 인증서 폐지목록 분산 관리 방법 중 인증시스템의 인증서 발급 과정에 대한 일실시예 흐름도.

도 7 은 본 발명에 따른 인증서 폐지목록 분산 관리 방법 중 실제 서비스 환경에서의 상대방 인증서의 유효성 검증 과정에 대한 일실사예 흐름도.

도 8 은 본 발명에 따른 인증서 폐지목록 분산 관리 방법 중 인증시스템의 특정 인증서 폐지 과정에 대한 일실시예 흐름도.

도 9 는 본 발명에 따른 인증서 폐지목록 분산 관리 방법에 이용되는 디렉토리 서버의 인증서 폐지목록 관리 구조에 대한 예시도.

* 도면의 주요 부분에 대한 부호의 설명

41 : 인증기관(CA) 42 : 디렉토리 서버

43 : 사용자 단말

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<13> 본 발명은 ITU-T(ITU-Telecommunication Standardization Sector) X.509에서 정의하고 있는 공개키 기반 구조(PKI : Public Key Infrastructure)의 보안 서비스 상에서 인증서 폐지목록(CRL : Certificate Revocation List)을 효과적으로 분산하여 관리하기 위한 인증서 폐지목록 분산 관리 방법과 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체에 관한 것이다.

<14> 공개키 기반 구조(PKI)는 인터넷과 같은 개방형 또는 분산형 정보통신망 환경에서 사용자 간에 주고받는 정보의 변경 여부를 확인하는 무결성, 사용자의 신분확인을 위한 인증, 사후 자신의 행위에 대한 부인방지 등에 필요한 공개키 암호방

식을 이용하는 보안서비스를 효과적으로 광범위하게 이용할 수 있도록 해주는 다수의 인증기관이 계층적으로 연결된 인증 메커니즘이라 할 수 있다.

<15> PKI에 대한 또 다른 표현으로는, 미국 IBM 사가 '인증서의 발행, 검증, 갱신, 취소, 등록의 관리, 키관리, 관련 서비스를 제공하는 인증기관, 등록기관, 저장소들의 시스템'으로, 캐나다 정부는 '거래 당사자간에 안전한 전자거래와 중요정보의 교환을 가능케하는 암호키와 인증서 전달시스템'으로 정의하고 있다. 따라서, PKI는 무결성, 인증, 부인방지 등의 보안서비스 제공을 위한 인증서의 생성, 처리 폐지 등의 과정과 전자서명 생성과 확인에 필요한 비밀키, 공개키 등의 각종 키를 관리하는 하드웨어, 소프트웨어, 정책들의 집합으로 볼 수 있다. 향후, PKI가 전자상거래, 은행, 증권, 보험 등 서로 다른 응용 분야나 환경, 인증기관간, 그리고 국제간에서 효율적으로 이용되려면 공개키 암호방식, PKI 관리 및 운영, 인증서 관련 규격, 인증 정책, 상호인증 등의 분야에서 국내 및 국제 표준화는 반드시 필요하다.

<16> 한편, ITU-T X.509에서는 인증 기관이 가입자에게 발급해 주는 인증서 규격에 대해 버전1(version 1, 이하 V1이라 함), 버전 2(version 2, 이하 V2라 함) 및 버전 3(version 3, 이하 V3라 함)을 정의하고 있다. 따라서, 본 발명과 관련된 인증서 폐지목록의 분배점 정보 구조체는 V3에서 정의한 인증서의 확장필드(즉, 첨부된 도 3a 참조)와 인증서 폐지목록 V2의 확장 필드(즉, 첨부된 도 3b 참조)와 관련된다.

<17> 이와 같이, 인증서 폐지목록을 효과적으로 관리하기 위한 ITU-T X.509 표준 문서에는 사전에 인증서 폐지목록에 분배점을 적용하기 위해서 필요한 기본 정보들을 정의하고 있지만, 구체적으로 어떤 방식으로 인증서 폐지목록에 분배점 메커니즘을 적용할 것인가에 관해서는 정의되어 있지 않다. 여기서, 인증서 폐지목록에 분배점 메커니즘이 적용

되지 않는 경우(도 1 참조)에 대한 일예를 도 2를 참조하여 상세히 살펴보면 다음과 같다.

<18> 도 2 는 도 1에 적용되는 사용자 단말 환경에서 인증서 폐지목록을 이용한 상대방 인증서의 유효성 검증 과정에 대한 상세 흐름도로서, 해당 가입자에게 적용하게 될 인증정책에서 인증서 폐지목록에 분배점을 적용하도록 설정이 되었는지를 검증하는 과정을 나타낸 것이다.

<19> 도 2에 도시된 바와 같이, 상대방 인증서에 대한 유효성을 검증하기 위해서는 사용자 단말은 해당 가입자로부터 상대방의 서브젝트 네임(SUBJECT_NAME)(이하, s라 칭함)을 입력받아(201) 상대방의 s를 사용하여 상대방 인증서에 관한 'LDAP_SEARCH' 구문을 작성한다(202).

<20> 이어서, 상기에서 작성된 구문을 사용하여 디렉토리 서버(204)로 상대방의 인증서를 요청하면(203) 디렉토리 서버(204)는 자신의 s를 이용하여 CRL에 관련된 'LDAP_SEARCH' 구문을 작성한다(205).

<21> 그리고, 작성된 구문을 사용하여 다시 디렉토리 서버로 CRL 파일을 전송할 것을 요청하면(206) 디렉토리 서버(204)는 전체 CRL 파일을 전달해준다(207).

<22> 그러면, 사용자 단말은 전달받은 CRL 파일을 기반으로 유효시간 범위를 체크하여(208), (205)과정에서 작성된 'LDAP_SEARCH' 구문을 이용해 상대방 인증서로부터 인증서의 일련번호를 추출하고(209), 해당 일련번호가 CRL에 있는지를 확인하여(210), 해당 일련번호가 CRL에 없으면 상대방 인증서의 유효성을 보장하고(211) 해당 일련번호가 CRL에 있으면 상대방 인증서가 비유효함을 인정한다(212).

<23> 따라서, 상기와 같은 종래 기술에서는 인증시스템에서 특정 가입자에 대한 인증서를 발급할 때, 인증서를 구성하는 맨더터리(mandatory) 필드 중의 하나인 서브젝트(SUBJECT)를 해쉬함수의 입력 데이터로 정의하여 서브젝트(SUBJECT)에 대응하는 해쉬함수의 결과값을 도출하여 이를 CRL의 DP 기준점으로 사용할 수 있도록 하는 방안이 필수적으로 요구된다.

【발명이 이루고자 하는 기술적 과제】

<24> 본 발명은, 상기한 바와 같은 요구에 부응하기 위하여 안출된 것으로, 분배점 메커니즘을 적용하여 인증서 폐지목록(CRL)을 효과적으로 분산 관리하기 위한 인증서 폐지목록 분산 관리 방법과 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공하는데 그 목적이 있다.

<25> 즉, 본 발명은, 인증시스템에서 발급하여 디렉토리 서버에서 상대방 인증서에 대한 유효성 정보를 담고 있는 인증서 폐기목록을 보안 서비스 사용자들이 효과적으로 검색할 수 있도록 하고, 디렉토리 서버로부터 사용자 단말환경으로 다운로드받는 CRL 파일 크기를 최소화시켜 보안서비스를 처리하는데 소요되는 시간을 줄이며, 특정 CRL 노드로의 집중적인 접근을 배제하여 N개의 CRL 노드에 균형(balance)있게 CRL 정보를 저장/관리하기 위한 인증서 폐지목록 분산 관리 방법과 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공하는데 그 목적이 있다.

【발명의 구성 및 작용】

<26> 상기 목적을 달성하기 위한 본 발명은, 인증서 폐지목록 분산 관리 시스템에 적용되는 인증서 폐지목록(CRL : Certificate Revocation List) 분산 관리 방법에 있어서, 상기 인증서 폐지목록의 분배구간을 산출하여 상기 인증서 폐지목록에 대한 인증정책을 등록하는 제 1 단계; 상기 등록된 인증정책에 따라 가입자 인증서를 구성하는 구조체를 셋팅하여 인증서를 발급하는 제 2 단계; 상기 발급된 인증서 폐지목록에 분배점 메커니즘을 적용하여 상대방 인증서의 유효성을 검증하는 제 3 단계; 및 사용자의 인증서를 폐지하기 위하여 상기 인증서 폐지목록의 분배점을 이용하여 인증서 폐지목록을 갱신하고, 그 내용을 게시하는 제 4 단계를 포함하여 이루어진 것을 특징으로 한다.

<27> 또한, 본 발명은, 프로세서를 구비한 인증서 폐지목록 분산 관리 시스템에, 상기 인증서 폐지목록의 분배구간을 산출하여 상기 인증서 폐지목록에 대한 인증정책을 등록하는 기능; 상기 등록된 인증정책에 따라 가입자 인증서를 구성하는 구조체를 셋팅하여 인증서를 발급하는 기능; 상기 발급된 인증서 폐지목록에 분배점 메커니즘을 적용하여 상대방 인증서의 유효성을 검증하는 기능; 및 사용자의 인증서를 폐지하기 위하여 상기 인증서 폐지목록의 분배점을 이용하여 인증서 폐지목록을 갱신하고, 그 내용을 게시하는 기능을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다

.

<28> 본 발명은, 인증시스템에서 발급하여 디렉토리 서버에서 상대방 인증서에 대한 유효성 정보를 담고 있는 인증서 폐기목록을 보안 서비스 사용자들이 효과적으로 검색할 수 있도록 하고, 디렉토리 서버로부터 사용자 단말환경으로 다운로드 받는 CRL 파일 크기를 최소화시켜 전송시간 단축과 그에 따른 가입자 단말 환경에서 보안서비스를 처리하

는데 소요되는 시간을 최소화할 수 있는 방안을 제공하며, 디렉토리 서버 측면에서 특정 CRL 노드로의 집중적인 접근을 배제하여 N개의 CRL 노드에 균형(balance)있게 CRL 정보를 저장/관리하여 궁극적으로 인증서 폐지목록 사용에 따른 제반의 비용을 절감시키는 것을 특징으로 한다.

<29> 상술한 목적, 특징들 및 장점은 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해 질 것이다. 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 일실시예를 상세히 설명한다.

<30> 도 4 는 본 발명이 적용되는 공개키 기반 구조(PKI : Public Key Infrastructure) 보안 서비스 시스템에 대한 구성예시도이다.

<31> 도 4에 도시된 바와 같이, 공개키 기반 구조(PKI : Public Key Infrastructure) 보안 서비스 시스템은, 가입자의 인증서 발급/폐지/재발급 업무를 수행하여 디렉토리 서버(42)로 인증서와 인증서 폐지목록을 게시/삭제하기 위한 인증기관(혹은 인증시스템, CA)(41)과, 인증기관(41)이 게시한 인증서/CRL을 서비스 가입자들이 참조할 수 있도록 해당 파일들을 관리하기 위한 디렉토리 서버(42)와, 인증기관(41)으로 사용자 인증서 발급/폐지를 요청하고, 서비스 처리시 디렉토리 서버(42)로 접근하여 상대방 인증서와 CRL을 다운로드받아 단말환경에서 보안 서비스를 처리하기 위한 사용자 단말(43)을 구비한다.

<32> 도 5 는 본 발명에 따른 인증서 폐지목록 분산 관리 방법 중 인증시스템의 인증정책(CPS : Certificate Policy Statement) 등록 과정에 대한 일실시예 흐름도이다.

<33> 도 5에 도시된 바와 같이, CA에서 CRL과 관련된 인증정책을 등록하기 위해서는, 먼

저 인증시스템에서 예상되는 가입자 수를 기반으로 인증서 폐지목록을 관리하게 될 DIT(Directory Information Tree, 이하 DIT)의 노드 수(number of nodes in DIT, 이하 N이라 칭함)와 해쉬함수(H())를 정의한다(501). 여기서, N은 CA에서 관리하고자 하는 CRL 파일의 개수를 말하고, H()는 CA에서 사용할 해쉬함수를 말한다.

<34> 이어서, 가입자 인증서를 구성하는 기본 항목 중의 하나인 서브젝트 네임(SUBJECT_NAME, 이하 S라 함)을 (501)과정에서 정의한 해쉬함수의 입력값으로 정의한다(502).

<35> 이후, (501,502)과정을 통해 정의된 함수 및 변수값들을 이용하여 인증서 폐지목록의 분배 구간을 산출한다(503). 이를 수식으로 나타내면 다음의 [수학식1] 및 [수학식2]와 같다.

<36> 【수학식 1】

$$H(S) = I$$

<37> 【수학식 2】

$$\frac{Vmax - Vmin}{N} = I$$

<38> 즉, [수학식1]과 같이 해쉬함수 H()에 S를 대입하여 얻을 수 있는 값을 V로 정의하였을 때, 최대치인 Vmax와 최소치인 Vmin간의 차이를 구하고, 이를 N으로 나누었을 때 얻어지는 값을 인증서 폐지목록의 분배구간값인 I로 정의한다.

<39> 그리고 나서, 인증서 폐지목록에 대한 인증정책 등록시, 인증서 폐지목록에 대한 분배점 메커니즘을 적용함을 알리기 위해 해당 변수값(예: crl_dp_flag)을 'yes'로 셋팅한 후(504), 기타 인증정책 등록을 진행한다(505).

<40> 도 6 은 본 발명에 따른 인증서 폐지목록 분산 관리 방법 중 인증시스템의 인증서

발급 과정에 대한 일실시예 흐름도이다.

<41> 도 6에 도시된 바와 같이, CA에서 가입자의 인증서를 발급하기 위해서는 먼저 해당 가입자에게 적용될 인증정책에서 인증서 폐지목록에 분배점을 적용하도록 설정(crl_dp_flag=yes)이 되었는지를 확인하여(601) 이 내용이 설정되지 않았으면 그냥 스킵하고(602), 설정되었으면 해쉬함수의 입력값인 가입자의 서브젝트 네임(SUBJECT_NAME), 즉 S를 추출한다(603).

<42> 이어서, 추출된 S에 대한 해쉬값, 즉 Vtmp를 추출한다(Vtmp=H(S))(604).

<43> 이후, (605)에서 (607)과정을 통해 (604)과정에서 얻어진 Vtmp가 포함되는 구간값을 추출한다. 이때, (608)에서 (610) 과정에서 인증서 폐지목록의 DN(Distingushied Name)체계를 OU(Organization Unit)는 CRLDP(n)으로, O(Organization)는 SECURITY로, C(Country)는 kr로 부여한다(608,609,610,611).

<44> 즉, (605)과정에서 (607)과정은 n값을 구하는 것이다. 또한, (608,609,610,611)과정은 (605)에서(607)과정을 통해 얻은 인증서 폐지목록의 구간값, 즉 n을 구하여 해당 인증서가 폐지되었을 때, 그 정보가 저장될 인증서 폐지목록의 DN을 완성시키는 것이다.

<45> 이후, (608,609,610,611)과정을 통해서 정해진 인증서 폐지목록의 DN과 인증서 폐지목록을 발급하는 인증기관의 DN 정보를 도 3a에 도시된 바와 같이, 분배점이름(DistributionPointName) 구조체를 구성하는 풀네임(fullName)과 CRL을 발급하는 CA의 이름(nameRelativeToCRLIssuer)에 채워, 해당 가입자의 인증서 구조체에 분배점이 적용된 가입자의 인증서 폐지목록 정보를 완성시킨다(612).

<46> 도 7 은 본 발명에 따른 인증서 폐지목록 분산 관리 방법 중 실제 서비스 환경에서

의 상대방 인증서의 유효성 검증 과정에 대한 일실시예 흐름도이다.

<47> 도 7에 도시된 바와 같이, 상대방 인증서에 대한 유효성을 검증하기 위해서는 먼저 응용프로그램이나 가입자로부터 상대방의 서브젝트 네임(SUBJECT_NAME)을 입력받아(701) 상대방 인증서에 관한 'LDAP_SEARCH' 구문을 작성한다(702). 이어서, 상기에서 작성된 구문을 사용하여 디렉토리 서버(704)로 상대방의 인증서를 요청하면(703) 디렉토리 서버(704)는 s를 이용하여 다운로드 받은 상대방 인증서로부터 해당되는 도 3a에 도시된 CRL분배점(crlDistributionPoint) 정보를 추출한다(705).

<48> 그리고, 성공적으로 추출된 CRL분배점(crlDistributionPoint) 정보에서 풀네임(fullname)을 추출하여 디렉토리 서버(704)로 CRL을 전송해줄 것을 요청하면(706) 디렉토리 서버(704)는 CRL분배점(crlDistributionPoint)에서 정의된 해당 DN의 이름이 부여된 CRL 파일을 전달해준다(707).

<49> 그러면, 사용자 단말은 전달받은 CRL 파일을 기반으로 유효시간 범위를 체크하여(708), (705)과정에서 추출된 CRL분배점(crlDistributionPoint) 정보를 이용해 상대방 인증서로부터 인증서의 일련번호를 추출하고(709), 해당 일련번호가 CRL에 있는지를 확인하여(710) 해당 일련번호가 CRL에 없으면 상대방 인증서의 유효성을 보장하고(711), 해당 일련번호가 CRL에 있으면 상대방 인증서가 비유효함을 인정한다(712).

<50> 도 8 은 본 발명에 따른 인증서 폐지목록 분산 관리 방법 중 인증시스템의 특정 인증서 폐지 과정에 대한 일실시예 흐름도로서, 인증서 폐지목록의 분배점을 이용하여 적합한 인증서 폐지목록을 갱신하고, 그 내용을 디렉토리 서버에 적절하게 게시하는 과정에 대한 것이다.

<51> 도 8에 도시된 바와 같이, CA가 사용자의 인증서를 폐지하기 위해서는 먼저 해당 가입자에게 적용된 인증정책에서 인증서 폐지목록에 분배점을 적용하도록 설정(crl_dp_flag=yes)이 되었는지를 확인하여(801) 이 내용이 설정되지 않았으면 그냥 스킵하고(802), 설정되었으면 인증서 폐지를 요청한 가입자의 인증서를 인증시스템의 데이터베이스(DB)로부터 로드시킨다(803).

<52> 이어서, 로드된 가입자 인증서로부터 CRL분배점(crlDistributionPoint) 정보를 추출하고, 이로부터 다시 분배점(DistributionPoint) -> 분배점네임(DistributionPointName) -> 풀네임(fullName)을 추출한다(804). 그리고, 추출된 분배점(DistributionPoint) -> 분배점네임(DistributionPointName) -> 풀네임(fullName)의 이름이 부여된 인증서 폐지목록 파일을 해당 인증시스템 데이터베이스(806)를 통해 검색하고(805), 검색된 분배점(DistributionPoint) -> 분배점네임(DistributionPointName) -> 풀네임(fullName)의 이름이 부여된 인증서 폐지목록 파일을 해당 데이터베이스(806)를 통해 로드시킨다(807).

<53> 이후, (803)과정을 통해 로드된 가입자의 인증서에서 일련번호를 추출하고 인증서를 폐지하는 사유를 가입자가 보낸 패킷으로부터 추출하고(808), (807)과정에서 로드된 해당 CRL에 해당 가입자 인증서의 일련번호와 폐기사유에 해당하는 코드를 추가하여(809) 해당 CRL 파일을 디렉토리 서버에서 관리하는 DIT의 적정한 노드에 게시하도록 한다(810).

<54> 상기와 같이, 본 발명에 대한 인증서 폐지목록에 분배점 메커니즘을 적용하면 도 9에 나타낸 바와 같이 디렉토리 서버에 N개의 노드로 균형있게 분산 관리된다.

<55> 즉, 본 발명은 인증시스템에서 발급하여 디렉토리 서버로 개시하는 CRL에 효과적인 DP 메커니즘을 적용함으로써, 보안 서비스 사용자들이 디렉토리 서버에서 상대편 가입자의 인증서 유효 정보가 저장된 CRL을 효과적으로 검색하여 사용자 단말환경으로 다운로드받는 CRL 크기를 최소화시키고, 가입자 단말환경에서 보안을 시행하는데 걸리는 시간을 최소화시키며, N 개의 CRL 노드에 균형있게 CRL 정보를 저장 및 관리하여 특정 노드로의 집중적인 접근을 배제시킨다.

<56> 이상에서 설명한 본 발명은 전술한 실시예 및 첨부된 도면에 의해 한정되는 것이 아니고, 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하다는 것이 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 있어 명백할 것이다.

【발명의 효과】

<57> 상기한 바와 같은 본 발명은, 첫째로 보안 서비스 사용자 관점에서 보면 디렉토리 서버로부터 사용자 단말환경으로 다운로드받는 CRL의 크기가 적기 때문에, 상대방 인증서의 유효성을 검증하는 시간을 단축시킬 수 있고 사용자 단말환경에서 보안 서비스를 처리하는 시간을 단축시킬 수 있는 효과가 있다.

<58> 두번째로, 디렉토리 서버 관점에서 보면 한 개의 파일로 관리하던 CRL을 여러 파일, 즉 여러 노드로 균형(balance)있게 분산 관리할 수 있으므로 특정 CRL 노드로의 집중적인 접근을 배제할 수 있는 효과가 있다.

<59> 세번째로, 인증 시스템 관점에서 보면 DP 메커니즘은 CRL이 다수의 CRL로 분리되고

그 크기가 균일하기 때문에 인증시스템에서 관리하는 데이터베이스에서 효과적으로 관리할 수 있을 뿐만 아니라 다양한 포멧의 사용자 이름을 수용할 수 있는 효과가 있다.

【특허청구범위】

【청구항 1】

인증서 폐지목록 분산 관리 시스템에 적용되는 인증서 폐지목록(CRL : Certificate Revocation List) 분산 관리 방법에 있어서,

상기 인증서 폐지목록의 분배구간을 산출하여 상기 인증서 폐지목록에 대한 인증정책을 등록하는 제 1 단계;

상기 등록된 인증정책에 따라 가입자 인증서를 구성하는 구조체를 셋팅하여 인증서를 발급하는 제 2 단계;

상기 발급된 인증서 폐지목록에 분배점 메커니즘을 적용하여 상대방 인증서의 유효성을 검증하는 제 3 단계; 및

사용자의 인증서를 폐지하기 위하여 상기 인증서 폐지목록의 분배점을 이용하여 인증서 폐지목록을 갱신하고, 그 내용을 게시하는 제 4 단계

를 포함하는 인증서 폐지목록 분산 관리 방법.

【청구항 2】

제 1 항에 있어서,

상기 제 1 단계는,

인증시스템에서 예상되는 가입자 수를 기반으로 인증서 폐지목록을 관리하게 될 DIT(Directory Information Tree)의 노드 수(number of nodes in DIT, 이하 N이라 칭함)와 해쉬함수(H())를 정의하는 제 5 단계;

상기 가입자 인증서를 구성하는 기본 항목 중 서브젝트 네임(SUBJECT_NAME)을 해쉬 함수의 입력값으로 정의하는 제 6 단계;

상기 정의된 함수 및 변수값들을 이용하여 인증서 폐지목록의 분배 구간을 산출하는 제 7 단계; 및

상기 산출된 값을 통해 인증서 폐지목록에 대한 해당 변수값(crl_dp_flag)을 셋팅하는 제 8 단계

를 포함하는 인증서 폐지목록 분산 관리 방법.

【청구항 3】

제 1 항에 있어서,

상기 제 2 단계는,

해당 가입자에게 적용될 인증정책에서 인증서 폐지목록에 분배점을 적용하도록 설정(crl_dp_flag=yes)이 되었는지를 확인하여 이 내용이 설정되지 않았으면 스킵하고, 설정되었으면 해쉬함수의 입력값인 가입자의 서브젝트 네임(SUBJECT_NAME)을 추출하는 제 5 단계;

상기 추출된 서브젝트 네임(SUBJECT_NAME)에 대한 해쉬값(Vtmp)을 추출하는 제 6 단계;

상기 추출된 해쉬값(Vtmp)에 따라 상기 해쉬값이 포함되는 구간값(n)을 추출하거나 상기 추출된 구간값(n)을 구하여 해당 인증서가 폐지되었을 때, 그 정보가 저장될 인증서 폐지목록의 DN(Distingushied Name)을 완성시키는 제 7 단계; 및

상기 인증서 폐지목록의 DN을 완성시킨 후에, 정해진 인증서 폐지목록의 DN 정보와 인증서 폐지목록을 발급하는 인증기관의 DN 정보를 이용하여 가입자 인증서를 구성하는 구조체를 셋팅하여 인증서를 발급하는 제 8 단계

를 포함하는 인증서 폐지목록 분산 관리 방법.

【청구항 4】

제 1 항 내지 제 3 항 중 어느 한 항에 있어서,

상기 제 3 단계는,

가입자로부터 상대방의 서브젝트 네임(SUBJECT_NAME)을 입력받아 상대방 인증서에 관한 구문을 작성하는 제 9 단계;

상기 작성된 구문을 사용하여 디렉토리 서버로 상대방의 인증서를 요청하고, 상기 요청에 따라 서브젝트 네임(SUBJECT_NAME)을 이용하여 다운로드받은 상대방 인증서로부터 해당 구조체에 관한 정보를 추출하는 제 10 단계;

상기 추출된 정보를 이용하여 상기 디렉토리 서버로 인증서 폐지목록 전송을 요청하고, 상기 요청에 따라 해당 DN의 이름이 부여된 상기 인증서 폐지목록을 전송받는 제 11 단계;

상기 전송받은 인증서 폐지목록을 기반으로 유효시간 범위를 체크하여, 상대방 인증서로부터 인증서의 일련번호를 추출하는 제 12 단계; 및

상기 해당 일련번호가 인증서 폐지목록에 있는지를 확인하여 해당 일련번호가 인증서 폐지목록에 없으면 상대방 인증서의 유효성을 보장하고, 해당 일련번호가 인증서 폐

지목록에 있으면 상대방 인증서가 비유효함을 인정하는 제 13 단계

를 포함하는 인증서 폐지목록 분산 관리 방법.

【청구항 5】

제 4 항에 있어서,

상기 제 4 단계는,

상기 가입자에게 적용된 인증정책에서 인증서 폐지목록에 분배점을 적용하도록 설정(crl_dp_flag=yes)이 되었는지를 확인하여 이 내용이 설정되지 않았으면 스킵하고, 설정되었으면 인증서 폐지를 요청한 가입자의 인증서를 데이터베이스(DB)에서 갱신하는 제 14 단계;

상기 갱신된 가입자 인증서로부터 구조체에 관한 정보를 추출하여 이름이 부여된 인증서 폐지목록을 해당 데이터베이스를 통해 검색하고, 검색된 인증서 폐지목록을 해당 데이터베이스를 통해 갱신하는 제 15 단계;

상기 갱신된 가입자의 인증서에서 일련번호를 추출하고 인증서를 폐지하는 사유를 가입자가 보낸 패킷으로부터 추출하는 제 16 단계; 및

상기 제 15 단계에서 갱신된 해당 인증서 폐지목록에 해당하는 가입자 인증서의 일련번호와 폐기사유에 해당하는 코드를 추가하여 해당하는 인증서 폐지목록을 상기 디렉토리 서버에서 관리하는 DIT(Directory Information Tree)의 노드에 게시하는 제 17 단계

를 포함하는 인증서 폐지목록 분산 관리 방법.

【청구항 6】

프로세서를 구비한 인증서 폐지목록 분산 관리 시스템에,

상기 인증서 폐지목록의 분배구간을 산출하여 상기 인증서 폐지목록에 대한 인증정책을 등록하는 기능;

상기 등록된 인증정책에 따라 가입자 인증서를 구성하는 구조체를 셋팅하여 인증서를 발급하는 기능;

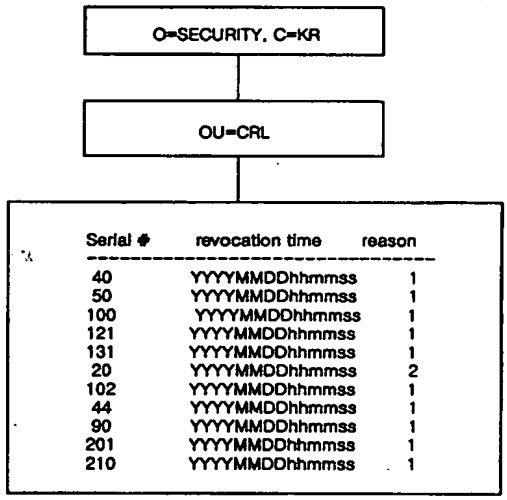
상기 발급된 인증서 폐지목록에 분배점 메커니즘을 적용하여 상대방 인증서의 유효성을 검증하는 기능; 및

사용자의 인증서를 폐지하기 위하여 상기 인증서 폐지목록의 분배점을 이용하여 인증서 폐지목록을 갱신하고, 그 내용을 게시하는 기능

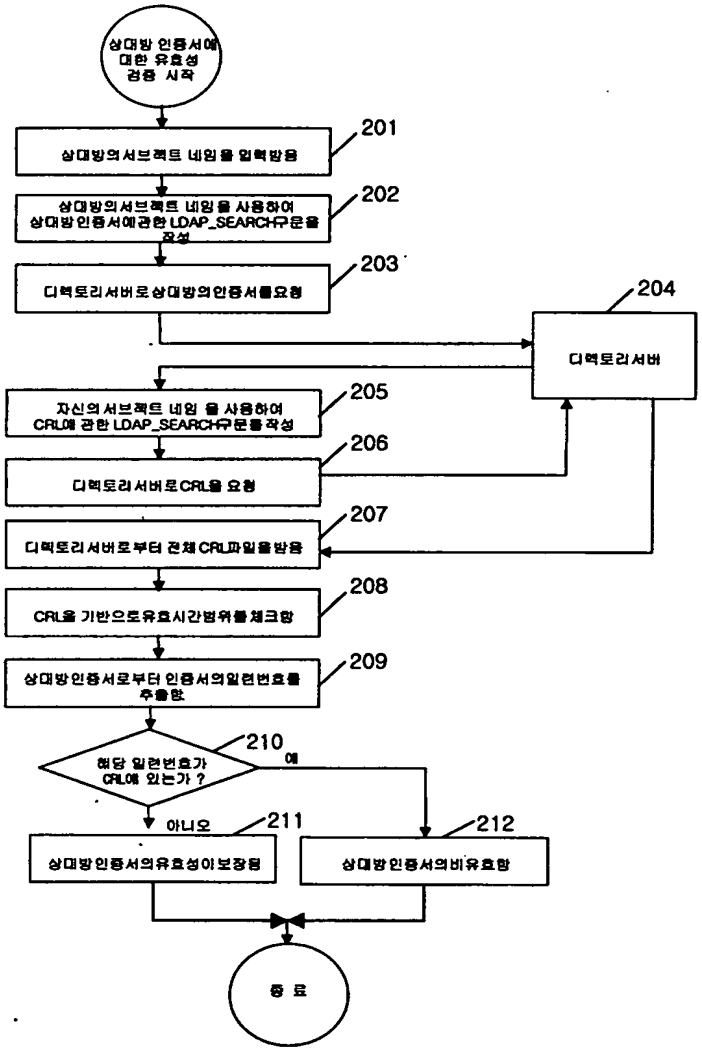
을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

【도면】

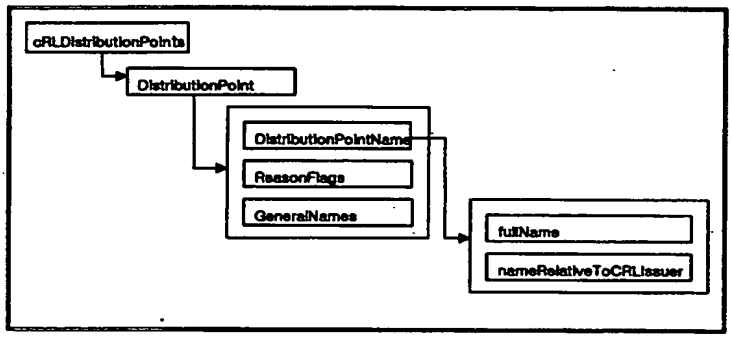
【도 1】


O=SECURITY, C=KR
OU=CRL
Serial # revocation time reason
40 YYYYMMDDhhmmss 1
50 YYYYMMDDhhmmss 1
100 YYYYMMDDhhmmss 1
121 YYYYMMDDhhmmss 1
131 YYYYMMDDhhmmss 1
20 YYYYMMDDhhmmss 2
102 YYYYMMDDhhmmss 1
44 YYYYMMDDhhmmss 1
90 YYYYMMDDhhmmss 1
201 YYYYMMDDhhmmss 1
210 YYYYMMDDhhmmss 1

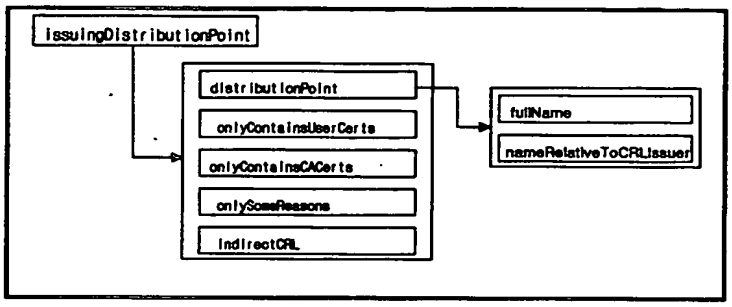
【도 2】


상대방 인증서에 대한 유효성 검증 시작
201
상대방의서브젝트 네임을 입력받음
202
상대방의서브젝트 네임을 사용하여 상대방인증서에관한 LDAP_SEARCH구문을 작성
203
디렉토리서버로상대방의인증서를요청
204
디렉토리서버
205
자신의서브젝트 네임 을 사용하여 CRL에 관한 LDAP_SEARCH구문을작성
206
디렉토리서버로CRL을 요청
207
디렉토리서버로부터 전체CRL파일을받음
208
CRL을 기반으로유효시간범위를체크함
209
상대방인증서로부터 인증서의일련번호를 추출함
210
해당 일련번호가 CRL에 있는가 ?
예
아니오
211
상대방인증서의유효성이보장됨
212
상대방인증서의비유효함
종 료

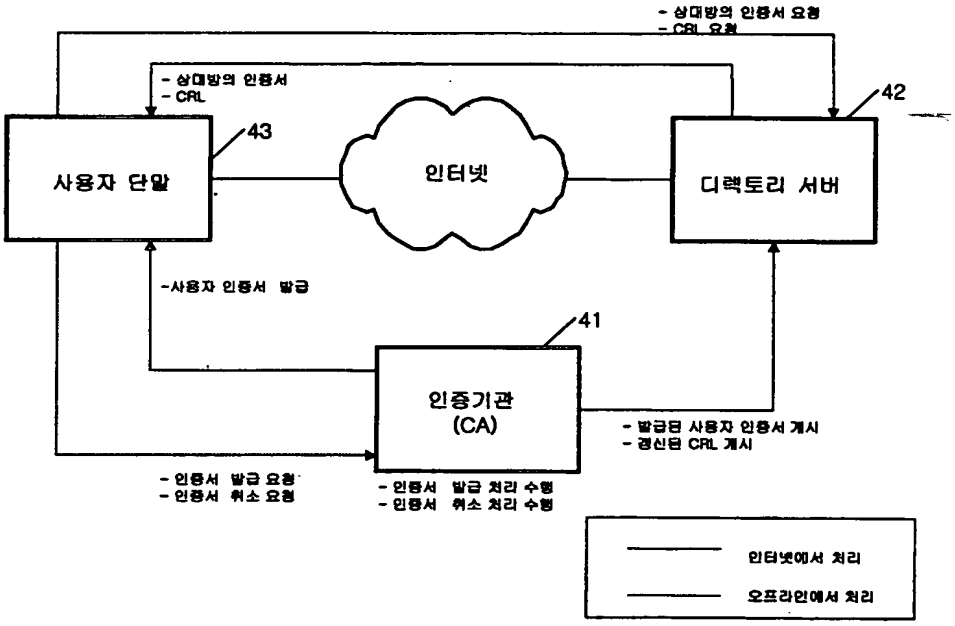
【도 3a】


cRLDistributionPoints
DistributionPoint
DistributionPointName
ReasonFlags
GeneralNames
fullName
nameRelativeToCRLIssuer

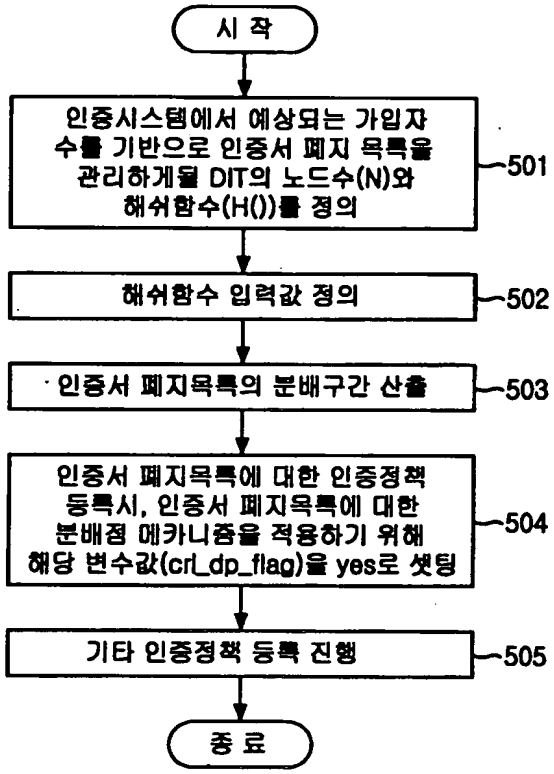
【도 3b】


issuingDistributionPoint
distributionPoint
onlyContainsUserCerts
onlyContainsCACerts
onlySomeReasons
indirectCRL
fullName
nameRelativeToCRLIssuer

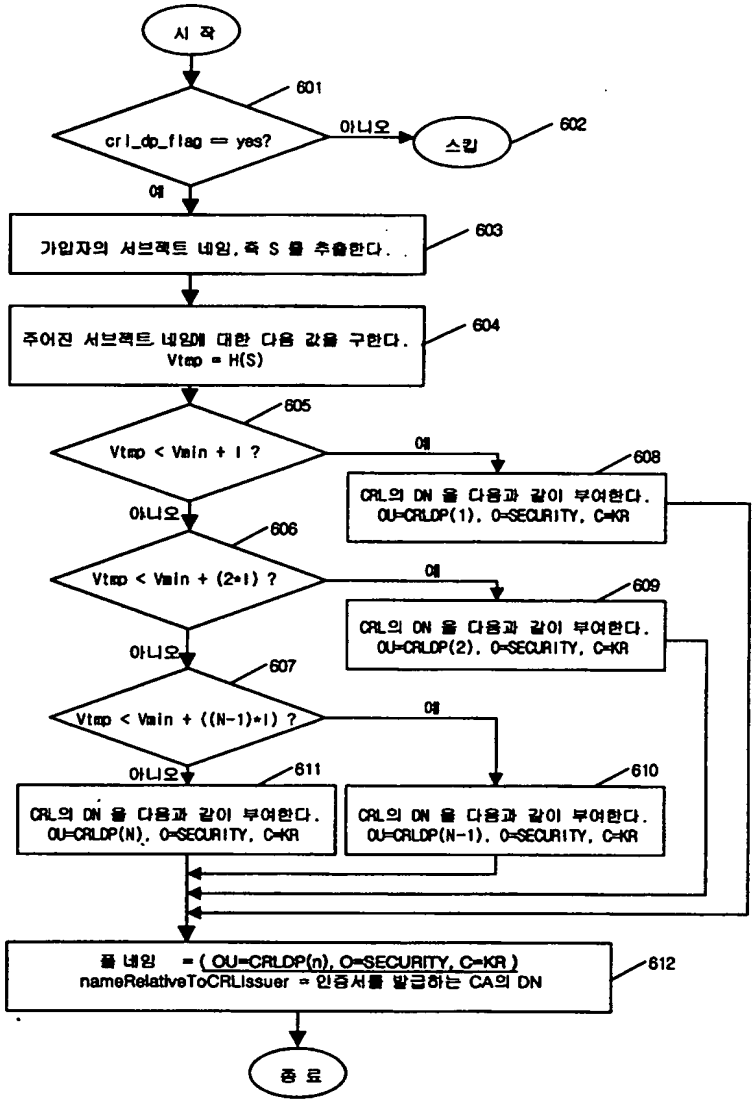
【도 4】


- 상대방의 인증서 요청
- CRL 요청
- 상대방의 인증서
- CRL
42
43
사용자 단말
인터넷
디렉토리 서버
-사용자 인증서 발급
41
인증기관
(CA)
- 발급된 사용자 인증서 게시
- 갱신된 CRL 게시
- 인증서 발급 요청
- 인증서 취소 요청
- 인증서 발급 처리 수행
- 인증서 취소 처리 수행
인터넷에서 처리
오프라인에서 처리

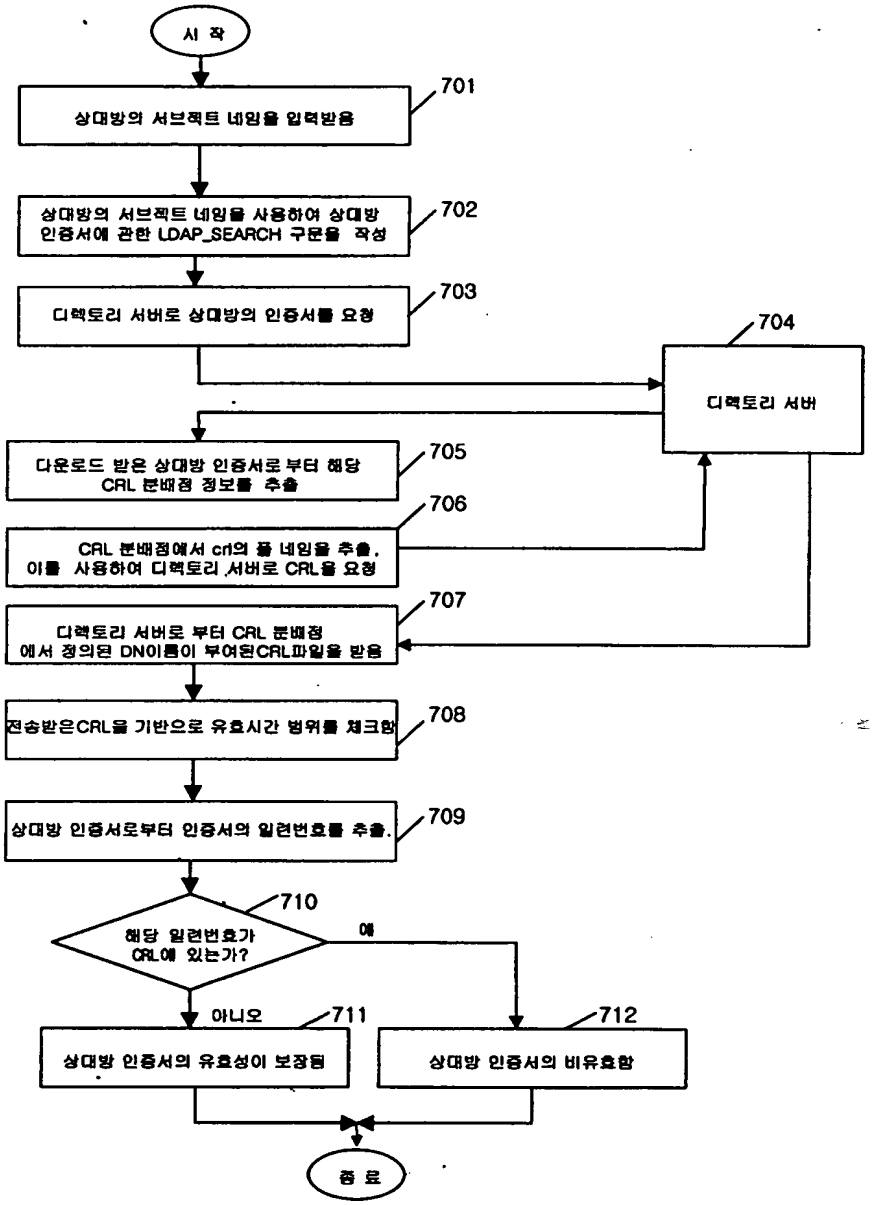
【도 5】


시 작
인증시스템에서 예상되는 가입자 수를 기반으로 인증서 폐지 목록을 관리하게될 DIT의 노드수(N)와 해쉬함수(H())를 정의
501
해쉬함수 입력값 정의
502
인증서 폐지목록의 분배구간 산출
503
인증서 폐지목록에 대한 인증정책 등록시, 인증서 폐지목록에 대한 분배점 메카니즘을 적용하기 위해 해당 변수값(crl_dp_flag)을 yes로 셋팅
504
기타 인증정책 등록 진행
505
종 료

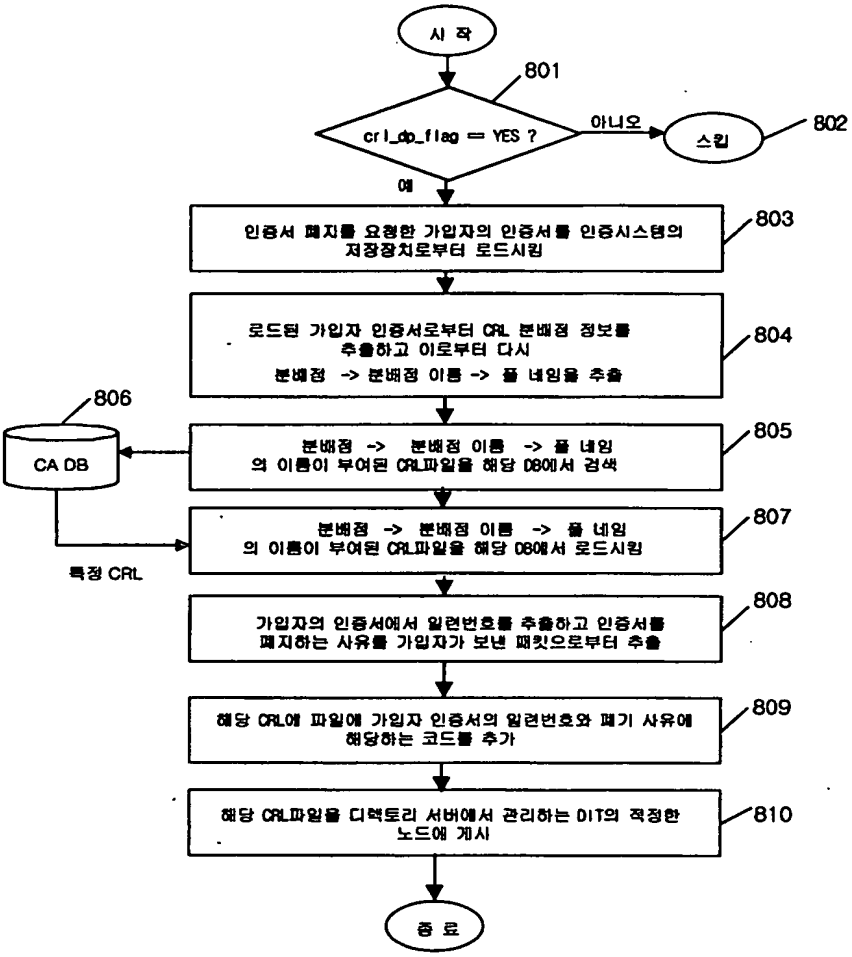
【도 6】


시 작
601
crl_dp_flag == yes?
아니오
스킵
602
예
가입자의 서브젝트 네임, 즉 S 를 추출한다.
603
주어진 서브젝트 네임에 대한 다음 값을 구한다.
Vtmp = H(S)
604
605
Vtmp < Vmin + I ?
예
608
CRL의 DN 을 다음과 같이 부여한다.
OU=CRLDP(1), O=SECURITY, C=KR
아니오
606
Vtmp < Vmin + (2*I) ?
예
609
CRL의 DN 을 다음과 같이 부여한다.
OU=CRLDP(2), O=SECURITY, C=KR
아니오
607
Vtmp < Vmin + ((N-1)*I) ?
예
아니오
611
CRL의 DN 을 다음과 같이 부여한다.
OU=CRLDP(N), O=SECURITY, C=KR
610
CRL의 DN 을 다음과 같이 부여한다.
OU=CRLDP(N-1), O=SECURITY, C=KR
폴 네임 = (OU=CRLDP(n), O=SECURITY, C=KR)
nameRelativeToCRLIssuer = 인증서를 발급하는 CA의 DN
612
종 료

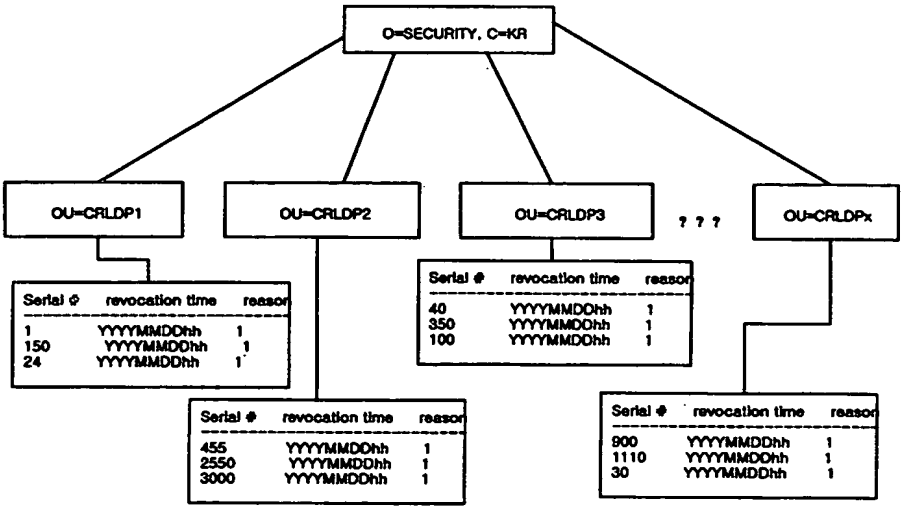
【도 7】


시 작
상대방의 서브젝트 네임을 입력받음
701
상대방의 서브젝트 네임을 사용하여 상대방 인증서에 관한 LDAP_SEARCH 구문을 작성
702
디렉토리 서버로 상대방의 인증서를 요청
703
704
디렉토리 서버
다운로드 받은 상대방 인증서로부터 해당 CRL 분배점 정보를 추출
705
CRL 분배점에서 cn의 풀 네임을 추출, 이를 사용하여 디렉토리 서버로 CRL을 요청
706
디렉토리 서버로 부터 CRL 분배점에서 정의된 DN이름이 부여된CRL파일을 받음
707
전송받은CRL을 기반으로 유효시간 범위를 체크함
708
상대방 인증서로부터 인증서의 일련번호를 추출.
709
해당 일련번호가 CRL에 있는가?
710
예
아니오
711
712
상대방 인증서의 유효성이 보장됨
상대방 인증서의 비유효함
종 료

【도 8】


시 작
801
crl_dp_flag == YES ?
아니오
스킵
802
예
인증서 폐지를 요청한 가입자의 인증서를 인증시스템의 저장장치로부터 로드시킴
803
로드된 가입자 인증서로부터 CRL 분배점 정보를 추출하고 이로부터 다시 분배점 -> 분배점 이름 -> 풀 네임을 추출
804
806
CA DB
분배점 -> 분배점 이름 -> 풀 네임의 이름이 부여된 CRL파일을 해당 DB에서 검색
805
분배점 -> 분배점 이름 -> 풀 네임의 이름이 부여된 CRL파일을 해당 DB에서 로드시킴
807
특정 CRL
가입자의 인증서에서 일련번호를 추출하고 인증서를 폐지하는 사유를 가입자가 보낸 패킷으로부터 추출
808
해당 CRL에 파일에 가입자 인증서의 일련번호와 폐기 사유에 해당하는 코드를 추가
809
해당 CRL파일을 디렉토리 서버에서 관리하는 DIT의 적정한 노드에 게시
810
종 료

【도 9】


O=SECURITY, C=KR
OU=CRLDP1
OU=CRLDP2
OU=CRLDP3
? ? ?
OU=CRLDPx
Serial # revocation time reasor
1 YYYYMMDDhh 1
150 YYYYMMDDhh 1
24 YYYYMMDDhh 1
Serial # revocation time reasor
40 YYYYMMDDhh 1
350 YYYYMMDDhh 1
100 YYYYMMDDhh 1
Serial # revocation time reasor
455 YYYYMMDDhh 1
2550 YYYYMMDDhh 1
3000 YYYYMMDDhh 1
Serial # revocation time reasor
900 YYYYMMDDhh 1
1110 YYYYMMDDhh 1
30 YYYYMMDDhh 1